

WHAT IS CLAIMED IS:

- 1 1. A multiply unit comprising:
2 at least one input data path for receiving one or more input operands to the multiply
3 unit;
4 an arithmetic multiplier connected to receive the one or more input operands;
5 a binary polynomial multiplier connected to receive the one or more input operands;
6 and
7 a multiply unit output data path connected to receive an output of the arithmetic
8 multiplier and connected to receive an output of the binary polynomial multiplier.
- 1 2. The multiply unit of claim 1, wherein the arithmetic multiplier includes a multiplier
2 array.
- 1 3. The multiply unit of claim 2, wherein the multiplier array is a Wallace tree multiplier
2 array.
- 1 4. The multiply unit of claim 2, wherein the multiplier array includes a plurality of
2 carry-save adders arranged in a tree structure.
- 1 5. The multiply unit of claim 4, further comprising a carry-propagate adder.
- 1 6. The multiply unit of claim 1, further comprising Booth recoding logic.
- 1 7. The multiply unit of claim 2, wherein the arithmetic multiplier performs 32-bit by 16-
2 bit multiplications in a two clock cycles.
- 1 8. The multiply unit of claim 2, wherein the arithmetic multiplier performs 32-bit by 32-
2 bit multiplications in three clock cycles.
- 1 9. The multiply unit of claim 1, wherein the binary polynomial multiplier includes a
2 binary polynomial multiplication array.

1 10. The multiply unit of claim 9, wherein the binary polynomial multiplier includes a
2 polynomial multiplication array having a first input and a second input, the polynomial
3 multiplication array including:

4 a plurality of row multipliers that multiply the first input by a bit of the second input;
5 and

6 at least one adder for computing a result by adding the results from the plurality of
7 row multipliers.

1 11. The multiply unit of claim 10, wherein the at least one adder performs a bitwise
2 exclusive-or on the results from the plurality of row multipliers.

1 12. The multiply unit of claim 10, wherein at least one of the plurality of row multipliers
2 performs multiplication by computing a logical AND of the first input and a bit of the second
3 input.

1 13. The multiply unit of claim 10 further comprising an accumulator, and wherein the at
2 least one adder computes a result by adding the results from the plurality of row multipliers
3 and the accumulator.

1 14. The multiply unit of claim 1 further comprising permutation logic.

1 15. In a processor core, a method for performing polynomial arithmetic, the method
2 comprising:

3 fetching an instruction to perform an operation from a data store;

4 reading one or more registers;

5 performing the operation using a multiply unit, the multiply unit comprising:

6 at least one input data path for receiving one or more input operands to the
7 multiply unit;

8 an arithmetic multiplier connected to receive the one or more input operands;

9 a binary polynomial multiplier connected to receive the one or more input operands;

10 and

11 a multiply unit output data path connected to receive an output of the arithmetic
12 multiplier and connected to receive an output of the binary polynomial multiplier.

1 16. The method of claim 15, wherein the arithmetic multiplier includes a multiplier array.

1 17 The method of claim 16, wherein the multiplier array is a Wallace tree multiplier
2 array.

1 18. The method of claim 16, wherein the multiplier array includes a plurality of carry-
2 save adders arranged in a tree structure.

1 19. The method of claim 18, the multiply unit further comprises a carry-propagate adder.

1 20. The method of claim 15, further comprising Booth recoding logic.

1 21. The method of claim 16, wherein the arithmetic multiplier performs 32-bit by 16-bit
2 multiplications in a two clock cycles.

1 22. The method of claim 16, wherein the arithmetic multiplier performs 32-bit by 32-bit
2 multiplications in three clock cycles.

1 23. The method of claim 15, wherein the binary polynomial multiplier includes a binary
2 polynomial multiplication array.

1 24. The method of claim 23, wherein the binary polynomial multiplier includes a
2 polynomial multiplication array having a first input and a second input, the polynomial
3 multiplication array including:

4 a plurality of row multipliers that multiply the first input by a bit of the second input;
5 and

6 at least one adder for computing a result by adding the results from the plurality of
7 row multipliers.

1 25. The method of claim 24, wherein the at least one adder performs a bitwise exclusive-
2 or on the results from the plurality of row multipliers.

1 26. The method of claim 24, wherein at least one of the plurality of row multipliers
2 performs multiplication by computing a logical AND of the first input and a bit of the second
3 input.

1 27. The method of claim 24, wherein the multiply unit further comprises an accumulator,
2 and wherein the at least one adder computes a result by adding the results from the plurality
3 of row multipliers and the accumulator.

1 28. The method of claim 15 wherein the multiply unit further comprises permutation
2 logic.

1 29. A computer-readable medium comprising a microprocessor core embodied in
2 software, the microprocessor core including a multiply-divide unit, the multiply-divide unit
3 comprising:

4 at least one input data path for receiving one or more input operands to the multiply
5 unit;

6 an arithmetic multiplier connected to receive the one or more input operands;

7 a binary polynomial multiplier connected to receive the one or more input operands;

8 and

9 a multiply unit output data path connected to receive an output of the arithmetic
10 multiplier and connected to receive an output of the binary polynomial multiplier.

1 30. The computer-readable medium of claim 29, wherein the arithmetic multiplier
2 includes a multiplier array.

1 31. The computer-readable medium of claim 30, wherein the multiplier array is a Wallace
2 tree multiplier array.

1 32. The computer-readable medium of claim 30, wherein the multiplier array includes a
2 plurality of carry-save adders arranged in a tree structure.

1 33. The computer-readable medium of claim 32, wherein the multiply unit further
2 comprises a carry-propagate adder.

1 34. The computer-readable medium of claim 29, further comprising Booth recoding
2 logic.

1 35. The computer-readable medium of claim 30, wherein the arithmetic multiplier
2 performs 32-bit by 16-bit multiplications in a two clock cycles.

1 36. The computer-readable medium of claim 30, wherein the arithmetic multiplier
2 performs 32-bit by 32-bit multiplications in three clock cycles.

1 37. The computer-readable medium of claim 29, wherein the binary polynomial
2 multiplier includes a binary polynomial multiplication array.

1 38. The computer-readable medium of claim 37, wherein the binary polynomial
2 multiplier includes a polynomial multiplication array having a first input and a second input,
3 the polynomial multiplication array including:

4 a plurality of row multipliers that multiply the first input by a bit of the second input;
5 and

6 at least one adder for computing a result by adding the results from the plurality of
7 row multipliers.

1 39. The computer-readable medium of claim 38, wherein the at least one adder performs
2 a bitwise exclusive-or on the results from the plurality of row multipliers.

1 40. The computer-readable medium of claim 38, wherein at least one of the plurality of
2 row multipliers performs multiplication by computing a logical AND of the first input and a

3 bit of the second input.

1 41. The computer-readable medium of claim 38, wherein the multiply unit further
2 comprises an accumulator, and wherein the at least one adder computes a result by adding the
3 results from the plurality of row multipliers and the accumulator.

1 42. The computer-readable medium of claim 29 wherein the multiply unit further
2 comprising permutation logic.